ДОГОВОР
О ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ ЮРИДИЧЕСКИХ ЛИЦ И ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ В ОАО «БАНК ЭСХАТА» (ПУБЛИЧНАЯ ОФЕРА)

Открытое акционерное общество «Банк Эсхата», именуемое в дальнейшем «Банк», с одной стороны, и Юридическое лицо или Индивидуальный предприниматель, действующий на основании законодательства, именуемый в дальнейшем «Клиент», с другой стороны, совместно именуемые «Стороны», а по отдельности «Сторона», заключили настоящий Договор дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в ОАО «Банк Эсхата» (далее – «Договор») с учетом условий и требований раздела 1 настоящего Договора:

1. ПОРЯДОК ЗАКЛЮЧЕНИЯ ДОГОВОРА

1.1. Настоящий Договор является публичной офертой и размещен на официальном сайте Банка www.eskhata.com, на странице входа в Систему дистанционного банковского обслуживания «Эсхата Бизнес» или на информационных стендах Банка и его структурных подразделений.

1.2. Акцептом настоящего Договора Клиентом является подача в Банк установленной Банком формы Заявки-запрос об акцепте публичной оферты (приложение № 1) в распечатанном виде с личной подписью и печатью или в случае наличия у Клиента расчетного счета, отправить Заявку-запрос через электроную почту на адрес электронной почты Банка указанной в Заявке.

1.3. Подтверждением заключения Договора является принятие Заявки-запроса и внесение отметки о его принятии уполномоченным лицом Банка или, проставление галочки в разделе «Ознакомлен и согласен с условиями оферты» через Систему дистанционного банковского обслуживания «Эсхата Бизнес» со стороны Клиента, имеющего расчетный счет в Банке. Один экземпляр Заявления-заявки, подписанный и заверенный печатью Клиента и с отметкой уполномоченного лица Банка, хранится в Банке, а второй экземпляр Заявления-заявки, с отметкой Банка предоставляется Клиенту по его требованию.

1.4. Акцепт настоящего Договора Клиентом является подтверждением того, что Клиент ознакомился с условиями настоящего Договора и Тарифов Банка. Клиент также подтверждает и соглашается соблюдать условия настоящего Договора и Тарифов Банка.

2. ПОНЯТИЯ И ТЕРМИНЫ

- **Акцеп-** признается ответ лица, которому адресована оферта.
- **НБТ -** Национальный банк Таджикистана.
- **аутентификация** –процедура, позволяющая кредитной организации удостоверить личность пользователя платёжной услуги или действительность прав на использование электронного платёжного средства, включая использование персонализированных защитных данных пользователей
- **Пользователь** – физическое лицо имеющий доступ к системе Эсхата Бизнес и наделенным определенным уровнем прав доступа со стороны Клиента (уполномоченное лицо Клиента, на чьё имя Банк предоставил логин и пароль).**учётная запись (аккаунт) -** совокупность данных пользователя в информационной системе Банка, необходимая для подтверждения его личности и предоставления доступа к его персональным данным и настройкам.».
- **электронный документ** – информация, которая представлена в электронной форме;
- **электронная форма** - совокупность технологий, позволяющие создавать, получать и обмениваться информацией путем применения электронной подписи;
- **номер телефона —** номер сотового телефона, предоставленный Клиенту оператором подвижной электросвязи в соответствии с договором на оказание услуг связи и предоставленный Клиентом Банку в качестве основного контактного номера для информационного и финансового взаимодействия с Банком посредством каналов Дистанционного обслуживания.
- **СМС уведомление –** отправка логина и пароля для входа или иной необходимой информации, связанной с Системой, через мобильные сети посредством SMS-сообщений пользователям Системы, номера телефонов которых были указаны Клиентом в Заявлении-заявке.

• **Авторизационные данные —** Коды доступа, уникальные логин (login), пароль (password) Клиента, а также другие данные, используемые для доступа и совершения операций через систему Эсхата Бизнес. Авторизационные данные являются аналогом собственноручной подписи (простой электронной подписью) уполномоченных лиц Клиента

• **простая электронная подпись** (ПЭП)- информация, дающая возможность определить участника электронного документооборота и его волю в действиях и сделках (договорах)

• **Логин-**уникальный псевдоним пользователя в программе дистанционного банковского обслуживания "Эсхата бизнес". Логин пользователю присваивается при регистрации пользователя в дистанционной банковской программе "Эсхата бизнес". Клиент может указать Логин пользователя самостоятельно (при условии, что указанный логин еще не существует в программе дистанционного банковского обслуживания "Эсхата бизнес");

• **Пароль (password)** - секретный набор символов, который вместе с логином обеспечивает доступ для входа клиента/пользователя в учетную запись (аккаунт) в программу дистанционного банковского обслуживания "Эсхата бизнес"

•

• **компрометация -** утрата, подозрение утраты, хищение, несанкционированное использование или копирование (подозрение на копирование) логина и пароля пользователя системы, либо ситуация, когда есть подозрения, что логин и пароль пользователя системы или другие авторизационные данные стали известны другому третьему лицу.

• **информационная система** – совокупность технических, программных и организационных средств для предоставления дистанционных банковских услуг

• **Google Authenticator** – программа обеспечивает двухфакторную аутентификацию для удаленного входа в систему и простых электронных подписей электронных документов с использованием алгоритмов одноразового пароля на основе времени (TOTP) и одноразового пароля на основе HMAC (HOTP). Эта программа реализует алгоритмы, указанные в RFC 6238 и RFC 4226.

• **аналог собственноручной подписи**– простая электронная подпись или иное средство идентификации, проставленное на электронный документе и признанное Сторонами для целей идентификации уполномоченных лиц Клиента.

• **дистанционные банковские услуги –**банковские услуги, предоставляемые клиентам с использованием электронных, программных, технических и телекоммуникационных средств без посещения кредитной организации;

Тариф — документ, содержащий информацию о размере и правилах применения, расчета, взимания и начисления процентов, комиссий, плат и штрафов. Тариф размещен на официальном сайте банка www.eskhata.com.

3. ПРЕДМЕТ ДОГОВОРА

3.1. Банк предоставляет юридическим лицам и индивидуальным предпринимателям услуги дистанционного банковского обслуживания через Систему дистанционного банковского обслуживания «Эсхата Бизнес» в веб-версии и мобильной версии (далее – «Система»).

На основании настоящего Договора и Договора (ов) банковского счета, заключенных между Банком и Клиентом, Банк предоставляет Клиенту услуги по приему и отправке электронных документов, обслуживанию в рамках зарплатного проекта, проведению банковских и иных операций, предусмотренных вышеуказанными договорами, внутренними банковскими нормативными документами и действующим законодательством. Клиент оплачивает стоимость услуг Банка в соответствии с Тарифами Банка и в установленном настоящим Договором порядке и Договора (ов) банковского счета.

3.2. Настоящий Договор устанавливает порядок подключения Клиента к Системе, условия предоставления услуг в Системе в соответствии с правилами и порядком дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей и Правила информационной безопасности при работе в системе дистанционного банковского обслуживания «Эсхата Бизнес» (далее – «Правила») и Тарифами Банка.

3.3. Подключение Клиента к Системе осуществляется на основании Заявки-запроса Клиента (Приложение № 1) в соответствии с условиями раздела 1 настоящего Договора.

3.4. Банк предоставляет данные услуги дистанционно через защищенную сеть Интернет в электронной форме на финансовом портале через официальный web-сайт Банка **https://business.eskhata.com** или в мобильной версии через мобильное приложение “Эсхата Бизнес” на условиях, указанных в настоящем Договоре.

4. ОБЩИЕ УСЛОВИЯ

4.1. Клиент может получить доступ к Системе дистанционного банковского обслуживания «Эсхата Бизнес» следующими способами и при условии соблюдения следующих требований:

4.1.1. Для входа в аккаунт в Систему через веб-версию необходим компьютер. Для мобильной версии требуется смартфон, планшет или другое электронное устройство с доступом в интернет.

4.1.2. Клиент должен войти в Систему по следующей ссылке **https://business.eskhata.com** или скачать мобильное приложение "Эсхата Бизнес" из Google play, App Store или других источников.
4.1.3. На странице входа в Систему Клиент использует логин и пароль, отправленные Банком на номер телефона или адрес электронной почты пользователя Системы, указанный в Заявлении-заявке.
4.1.4. Пользователь системы для смены пароля должен соблюдать требования, указанные на странице входа в систему, и требования Правил информационной безопасности при работе в системе дистанционного банковского обслуживания «Эсхата Бизнес» (Приложение 4).
4.1.5. Для следующей аутентификации пользователь Системы должен использовать свой логин и пароль.
4.2. Клиент должен выполнять требования Банка к структуре и форме аппаратного и программного обеспечения, необходимого для стабильной работы Системы. Эти требования следующие:
4.2.1. Для системы в веб-версии:

- Процессор – не ниже Intel Pentium IV;
- ОЗУ - не менее 128 MB;
- свободное место на диске не менее 50 Мб;
- доступ в Интернет;
- антивирусная защита и регулярное обновление антивирусных баз.

4.2.2. Для системы в мобильной версии:

- Смартфон, планшет или другое мобильное электронное устройство с операционной системой Android (версия не менее 8) и iOS.

4.3. Через Систему осуществляются следующие операции на основании следующих документов:

- платёжное поручение в национальной валюте;
- заявление на перевод денежных средств в иностранной валюте;
- заявление на покупку (продажу) иностранной валюты;
- заявление на конверсионные операции с одной валюты на другую;
- операции в рамках Зарплатного проекта;
- заявление на открытие дополнительного счета;
- заявление на открытие депозитного счета;
- заявление на получение кредита;
- иные документы, которые используются в зависимости от отношений между Клиентом и Банком, в соответствии с требованиями действующего законодательства Республики Таджикистан, нормативных актов НБТ и внутренних документов Банка.

Перечень операций и действий не является окончательным и может быть расширен по мере развития обслуживания или внедрения услуги в соответствии с требованиями нормативно-правовых актов, актов НБТ и внутренних документов Банка.
4.4. Обслуживание через Дистанционную систему осуществляется ежедневно (кроме выходных и праздничных дней) в течение рабочего дня установленного банком. Все операции и уведомления, проводимые в рамках данного договора, фиксируются по времени Душанбе. Клиент обязан учитывать возможные различия в часовом поясе при осуществлении операций.
4.5. Банк и Клиент признают, что принятие электронных документов, заверенных простой электронной подписью или аналогом собственноручной подписи с юридической точки зрения равнозначно документам на бумажном носителе с подписями, заверенными в карточке с образцами подписей и оттиском печати, а права и обязанности, вытекающие из таких документов, имеют такую же юридическую силу, как и документы на бумажном носителе. Все электронные документы, которыми Банк и Клиент обмениваются через Систему, могут быть использованы в качестве доказательств при разрешении споров.
4.5.1. В случае если карточка с образцами подписей и оттиска печати Клиента предусматривает только первую подпись, достаточным условием для оказания услуг с использованием Системы является получение логина, пароля одного из уполномоченных лиц Клиента с правом первой подписи.
4.5.2. В случае если карточка с образцами подписей и оттиска печати Клиента предусматривает наличие второй подписи, достаточным условием для оказания услуг с использованием Системы является получение следующих двух логинов и паролей:
-от одного из уполномоченных лиц Клиента с правом первой подписи;
-от одного из уполномоченных лиц Клиента с правом второй подписи.
Также, в соответствии с Заявлением-заявкой (Приложение № 1), определяется роль уполномоченных лиц Клиента, уполномоченным лицам предоставляется доступ к Системе «с правом первой подписи», «с правом второй подписи», «без права подписи для составления документов» и «без права подписи для просмотра информации».
4.5.3. Смена логина, пароля производится каждый раз при смене уполномоченного лица Клиента или при компрометации логина, пароля. Смена логина, пароля производится на основании Заявки одновременно с заменой карточки с образцами подписей и оттиска печати Клиента.
4.6. Стороны признают, что система защиты информации является достаточной для защиты от

несанкционированного вмешательства и подтверждения авторства и подлинности электронного документа, что делает невозможным потенциальное вмешательство третьих лиц.
4.7. Прием и предоставление электронных документов через Систему осуществляется в бумажном виде, за исключением случаев, когда Банк требует представления бумажных документов.
4.8. Банк оказывает Клиенту помощь в запуске Системы, подготавливает обучающий материал и предоставляет Клиенту, консультирует по вопросам использования Системы в течение срока действия настоящего Договора. Банк обеспечивает функционирование Системы в целях обеспечения безопасности операций, логинов и паролей.
4.9.
Принимая настоящий Договор, Клиент автоматически предоставляет свои банковские реквизиты (включая полное или сокращенное наименование, уникальный номер счета, идентификационный номер налогоплательщика (ИНН), банковский идентификационный номер (БИН) и другие данные) для их размещения на платформе дистанционной системы «Эсхата Бизнес» и в мобильном приложении «Эсхата Онлайн». Это необходимо для предоставления Плательщикам возможности осуществлять платежи на счет Клиента. Клиент выражает свое согласие с данным условием."

5. ПРАВА И ОБЯЗАННОСТИ СТОРОН

5.1. **Банк обязан:**
5.1.1 Осуществлять банковские операции на основе электронного документа Клиента в срок, указанный в Договоре банковского счета.
5.1.2. Не исполнять электронные документы Клиента, нарушающие требования действующего законодательства Республики Таджикистан, нормативных актов Национального банка Таджикистана и условия настоящего Договора, а также документы, не имеющие ПЭП или аналога собственноручной подписи или в случае их недостоверности. В случае нарушения требований законодательства по противодействию легализации (отмывания) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового поражения отказаться от исполнения поручения Клиента или расторгнуть договор.
5.1.3 По электронному запросу Клиента через Систему и обработанному комплексом защиты информации, используемым в рамках настоящего Договора, сформировать:

- уведомление о результате обработки каждого электронного документа путем изменения статуса этого документа;
- выписку по расчетному счету Клиента;
- и иные действия, которые позволит выполнить Система.

5.1.4. В случае получения от Клиента информации о компрометации (п. 5.2.5. настоящего Договора), с момента получения информации приостановить прием, отправку и исполнение электронных документов до выяснения ситуации. Также временно приостанавливается работа Системы Клиента по телефонному запросу Клиента при подтверждении Клиентом своих идентификационных данных.
5.1.5. В случае приостановки работы Системы, предоставить информацию об этом на сайте Банка и уведомить Клиента.
5.1.6. В случае необходимости на основании письменного заявления Клиента утвердить бумажную копию электронных документов, полученных Клиентом через Систему, подписанную уполномоченными лицами Банка и скрепленную печатью Банка в течение не более 3 (трех) рабочих дней.
5.1.7. Соблюдать конфиденциальность информации, связанной с использованием Системы, за исключением случаев, предусмотренных действующим законодательством Республики Таджикистан и условиями настоящего Договора.
5.1.8. Консультировать сотрудников Клиента по вопросам работы с Системой, предоставлять возможность пользоваться информационно-справочными, коммуникационными и другими услугами.
5.1.9. Обеспечивать хранение (архивирование) электронных документов в соответствии со сроками, установленными нормативными документами НБТ.
5.1.10. По истечении срока действия логин и пароля пользователей системы поменять их после принятия заявки Клиента.
5.1.11. Выслать на указанный Клиентом номер телефона или адрес электронной почты логин и пароль для входа в Систему после принятия Заявления-заявки Клиента.

5.2. Клиент обязан:
5.2.1. Соблюдать положения настоящего Договора и его приложения.
5.2.2 Формировать электронные документы с использованием Системы на основании первичного экземпляра оригинала документа.
5.2.3. Отправлять электронные документы через Систему, удостоверенные аналогом собственноручной подписи или простой электронной подписью.

5.2.4 Обеспечить конфиденциальность данных о логине и пароле, безопасность и защиту, а также предотвращение доступа третьих лиц. Не хранить логин, пароль и/или авторизационные данные на рабочем компьютере.
5.2.5 Немедленно уведомить по телефону Банк в случае механического повреждения носителя или компрометации назвав слово блокировать и указав время приостановки операций. Также подать в Банк заявку на смену логина и пароля в течение одного рабочего дня.
5.2.6 Предоставить электронные документы, направленные в Банк через Систему, на бумажном носителе в течение 5 (пяти) дней со дня принятия запроса Банка. Данные документы должны быть подписаны уполномоченными лицами Клиента и скреплены печатью Клиента.
5.2.7 В случае необходимости предоставления документов в соответствующие органы предоставить в Банк распечатанные копии документов для проставления печати Банка.
5.2.8. Хранить электронные документы, подписанные аналогом собственноручной подписи или простой электронной подписью, в соответствии с законодательством Республики Таджикистан и нормативными правовыми актами НБТ не менее 5 (пяти) лет.
5.2.9. В случае получения уведомления от Банка через Систему о замене программного обеспечения принять меры по своевременному принятию и внедрению нового программного обеспечения.
5.2.10. Незамедлительно сообщать Банку обо всех изменениях в карточке с образцами подписей и оттиском печати. Замена карточки с образцами подписей и оттиском печати является основанием для прекращения обмена информацией через Систему и изменения логина и пароля.
5.2.11. Не вносить изменения в программное обеспечение и техническую документацию, предоставляемую Банком по настоящему Договору, и не передавать его третьим лицам.
5.2.12. Оплатить стоимость дистанционного банковского обслуживания согласно Тарифам Банка.
5.2.13. Незамедлительно сообщать Банку об изменении номера телефона, адреса электронной почты, смене уполномоченного лица, имеющего доступ к Системе.
5.2.14. Обезопасить компьютер, смартфон, планшет или другое электронное устройство, через которое осуществляется работа в Системе, от вирусных атак или других вредоносных программ.

5.3. **Стороны обязаны:**

5.3.1 Ограничить доступ третьих лиц к программному обеспечению и техническим средствам и предоставить доступ к проведению операций только владельцам логина и пароля.
5.3.2 При компрометации осуществить внеплановую смену логина и пароля и одновременно прекратить электронный обмен данными.
5.3.3 В случае выхода из строя программно-технического обеспечения Системы или ее отдельных элементов, а также в случаях, когда предоставление (использование) услуги, указанной в Разделе 2 настоящего Договора, становится невозможным, что является основанием для приостановки пользования Системой, каждая сторона обязана в течение 1 (одного) рабочего дня уведомить другую Сторону любым доступным способом и в течение 2 (двух) рабочих дней направить письменную информацию о подготовке и сроках возобновления обмена электронными документами. В период приостановки использования Системы обмен документами осуществляется посредством бумажного носителя или иных средств связи, предусмотренных договором банковского счета.

5.4. **Банк имеет право:**

5.4.1. Требовать от Клиента смены логина, пароля в следующих случаях:
- плановая смена паролей;
- внеплановая смена паролей;
- сброс пароля по требованию Клиента;
- смена уполномоченных (пользователей) лиц Клиента;
- компрометация;
- при необходимости проведения регламентных работ, связанных с обслуживанием программных и аппаратных средств Системы.

5.4.2. Прекратить оказание услуг в случае обнаружения попыток сканирования, доступа третьих лиц к Системе, атак на информационные ресурсы Банка, а также в случае обнаружения иных признаков нарушения безопасности с использованием программных и аппаратных средств Клиента, либо неисполнение или ненадлежащее исполнение условий настоящего Договора, в том числе:
- отправка в Банк электронных документов с признаками нарушения требований защиты данных;
- разглашение логина и пароля третьим лицам независимо от причин;
- нарушение условий настоящего Договора или правил использования Системы.

5.4.3. Списать в безакцептном порядке со счета Клиента, открытого в Банке, суммы комиссий и платежей за услуги Банка, а также плату за дополнительные услуги;
5.4.4. Отказать в приеме электронных документов от Клиента в случае обнаружения подозрительных действий Клиента, предварительно направив ему соответствующее уведомление.

5.4.5. Отказать в приеме электронных документов, если они не соответствуют требованиям действующего законодательства.
5.4.6. Запросить у Клиента всю информацию и документы (договоры, квитанции об оплате или другие подтверждающие документы), которые связаны с исполнением предмета настоящего Договора в течение деловых отношений и в течение 5 лет после их прекращения.
5.4.7 В одностороннем порядке вносить изменения и дополнения в настоящий Договор или приложения к нему, а также в Тарифы Банка, и сообщать об изменениях, вносимых в одностороннем порядке (в том числе о введении в действие таких изменений) не позднее, чем за **5 (пять)** календарных дней до момента введения в действие таких изменений и дополнений. Информация доводится до сведения Клиента путем её размещения на информационных стендах Банка, либо путем размещения новой редакции Договора (приложений к нему) и Тарифов Банка, либо самих изменений и дополнений на официальном сайте Банка **www.eskhata.com** или в системе дистанционного банковского обслуживания;
5.4.8. Осуществлять видеонаблюдение и запись телефонных разговоров в своих помещениях и на своем оборудовании в целях обеспечения безопасности и улучшения качества услуг без дополнительного уведомления Клиента. Видеозаписи и телефонные разговоры в будущем могут быть использованы в качестве доказательств;
5.4.9. В целях формирования и повышения лояльности Клиента к банковским услугам проводить акции и маркетинговую рекламу, в рамках которых Клиенту рассылаются специальные предложения Банка;
5.4.10. Приостановить отдельные операции или все банковские операции в связи с техническим процессом банковского обслуживания (ремонт оборудования, установка программы, настройка программы, устранение дефектов оборудования или банковской программы и обстоятельств, не зависящих от Банка);
5.4.11. Проверить достоверность информации и документов, предоставленных Клиентом;
5.4.12. В одностороннем порядке блокировать доступ пользователей Системы в следующих случаях:
- неисполнение требований настоящего Договора и договора банковского счета;
- прекращение или истечение срока полномочий уполномоченного лица Клиента;
- по иным основаниям, установленным законодательством Республики Таджикистан или настоящим Договором.
5.4.13. Банк имеет право приостановить или прекратить использование Клиентом Системы в следующих случаях:
- по требованию уполномоченных государственных органов в порядке и обстоятельствах, предусмотренных законодательством Республики Таджикистан;
- при отсутствии обмена поручениями между Сторонами через Систему более 3 (трех) месяцев подряд;
- в случае непредоставления или неполного предоставления документов (данных) по запросу Банка в целях реализации требований законодательства по противодействию отмыванию доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового поражения;
- в случае получения уведомления о доступе третьих лиц к Системе и предоставления доступа к Системе третьим лицам со стороны Клиента.
5.4.14. Осуществлять иные права, предусмотренные настоящим Договором и законодательством Республики Таджикистан.

5.5. Клиент имеет право:
5.5.1. Требовать от Банка своевременного проведения банковских операций по отправленным электронным документам при условии, что оформленные документы соответствуют требованиям, предусмотренным настоящим Договором и правилами дистанционного банковского обслуживания.
5.5.2. Сменить свой пароль в любое время.
5.5.3. Отозвать ранее отправленный электронный документ с подлинным аналогом собственноручной подписи путем направления в Банк защищенной информации через Систему или в письменном виде (на бумажном носителе), при условии, что Банк не снял денежные средства со счета Клиента по предыдущему электронному документу.
5.5.4. Пользоваться Системой в соответствии с требованиями настоящего Договора.
5.5.5. Обращаться в Банк для смены логина и пароля, за технической помощью в рамках дистанционного банковского обслуживания.
5.5.6. Прекратить использование Системы в соответствии с требованиями, указанными в Договоре.
5.5.7. Получать и передавать электронные документы от/в Банк через Систему.
5.5.8. Временно приостанавливать работу Системы (доступ к ней уполномоченных лиц), позвонив в Банк в установленное рабочее время.
5.5.9. Осуществлять иные права, предусмотренные настоящим Договором и законодательством Республики Таджикистан.

6. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. Стороны несут ответственность за неисполнение или ненадлежащее исполнение условий настоящего Договора в соответствии с действующим законодательством.
6.2. В случае неисполнения Клиентом требований пункта 5.2.5. настоящего Договора Банк освобождается от ответственности за убытки, возникшие у Клиента в результате операций со счетами Клиента.
6.3. Ответственность за правильное оформление и своевременную отправку электронных документов полностью возлагается на Клиента. Банк освобождается от ответственности за задержку в исполнении поручения Клиента, возникшую в результате несвоевременной отправки или составления электронных документов, не соответствующих установленным требованиям.
6.4. Банк не несет ответственности за неправильное функционирование оборудования и программного обеспечения Клиента, которое сделало невозможным доступ Клиента к Системе, что привело к просрочке платежей Клиента, а также за возможную (частичную или полную) потерю данных, содержащихся на вычислительных устройствах Клиента, подключенных к сети Интернет для оказания услуг.
6.5 В случае возникновения между Банком и Клиентом споров, связанных с использованием Системы, Стороны обязуются урегулировать споры в соответствии с «Правилами проведения экспертизы в случае возникновения споров» (Приложение 3) и выполнять положения Правил.
6.6. Клиент несет ответственность за обеспечение безопасности программного и аппаратного обеспечения, используемого в Системе, обеспечение сохранности логина и пароля от доступа третьих лиц, а также обеспечение безопасности программного и аппаратного обеспечения от вирусных атак и любого вирусного программного обеспечения.
6.7. Клиент несет ответственность за безопасность и передачу данных Google Authenticator, которые используются для доступа в системе «Эсхата Бизнес».
6.7.1. Клиент обязан:
1. Обеспечить безопасность устройства, на котором установлен Google Authenticator.
2. При необходимости самостоятельно перенести Google Authenticator на новое устройство.
6.8. Банк не несет ответственности за:
- Потерю доступа к аккаунтам в случае утери или кражи устройства с Google Authenticator-ом;
- Некорректной работы Google Authenticator в результате действий Клиента.
6.9. Клиент несет ответственность за все виды операций, совершаемых с момента получения доступа к Системе**.**

7. ФОРС-МАЖОР

7.1 Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Договору, если оно явилось следствием чрезвычайных обстоятельств, возникших после подписания настоящего Договора и являющихся для сторон непредвиденными и непреодолимыми.
7.2 К чрезвычайным обстоятельствам относятся события, не зависящие от сторон и за которые они не несут ответственности, такие как наводнения, пожары, землетрясения, иные стихийные бедствия, повреждения линий связи, забастовки, военное положение, эпидемия, решения или распоряжения органов государственной власти, прямо или косвенно препятствующие выполнению обязательств по настоящему Договору.
7.3 Срок исполнения обязательств по настоящему Договору продлевается на время действия чрезвычайных обстоятельств.
7.4 Если указанные обстоятельства продолжаются более 30 (тридцати) календарных дней, каждая из сторон вправе отказаться от исполнения договорных обязательств, и в этом случае стороны освобождаются от права на возмещение возможного ущерба.
7.5 Сторона, находящаяся в чрезвычайной ситуации, обязана уведомить другую сторону в письменной или электронной форме, и по требованию другой стороны, предоставить документы, подтверждающие наличие такой ситуации выданные органами государственной власти.

8. РАЗРЕШЕНИЕ СПОРОВ И ПОРЯДОК РАССМОТРЕНИЯ ЖАЛОБ

8.1 В случае несвоевременного исполнения, грубого обращения и других действий со стороны сотрудников Банка, которые приводят к снижению качества обслуживания и нарушению прав Клиента, Клиент может обратиться в Банк по телефону **808** или по электронной почте: **shikoyat@eskhata.tj**.
8.2 Жалоба Клиента рассматривается в течение до 30 дней с момента ее поступления в Банк, по результатам которого Клиенту дается официальный ответ.
8.3 Ответ на письмо (заявление) Клиента направляется Банком одним из способов и методов, указанных во втором предложении пункта 5.4.7 настоящего Договора.
8.4. Все споры и разногласия, возникающие в связи с выполнением соответствующих разделов настоящего Договора, решаются путем переговоров.
8.5. В случае если споры не будут разрешены путем переговоров, стороны имеют право обратиться в суд с иском к другой стороне в соответствии с действующим законодательством Республики Таджикистан.
8.6. Применимым правом по договору является законодательство Республики Таджикистан.

9. ПОРЯДОК РАСЧЕТОВ

9.1 Оплата услуг Банка по технической поддержке Системы, а также взимание комиссии за проведение расчетов по счету с использованием Системы осуществляется в соответствии с Тарифами Банка.
9.2. Тарифы на услуги изменяются Банком в одностороннем порядке в соответствии с подпунктом 5.4.7 настоящего Договора.
9.3 Если Клиент не согласен с новыми Тарифами Банка, Клиент имеет право расторгнуть настоящий Договор в течение 5 (пяти) рабочих дней с даты вступления в силу Тарифов, направив письменное уведомление Банку.
9.4. Клиент поручает Банку без дополнительного распоряжения Клиента взимать плату за услуги Банка по технической поддержке Системы и другие дополнительные услуги со счета Клиента, а в случае недостаточности денежных средств на счете, с других счетов Клиента. Настоящим Клиент подтверждает, что поручение о списании платы за услуги с его Счета является предварительным акцептом Клиента.

10. СРОК ДЕЙСТВИЯ ДОГОВОРА И ПОРЯДОК ЕГО РАСТОРЖЕНИЯ

10.1 Настоящий Договор вступает в силу с момента его акцепта Клиентом и действует в течение неопределенного срока.
10.2. Стороны имеют право расторгнуть настоящий Договор в одностороннем порядке. Сторона, желающая расторгнуть Договор, должна направить другой Стороне письменное уведомление за 30 (тридцать) дней о своем намерении расторгнуть Договор.
10.3 Действие настоящего Договора прекращается в следующих случаях:
10.3.1. В случае расторжения договора банковского счета;
10.3.2. По заявлению Клиента при отсутствии задолженности перед Банком;
10.3.3. По инициативе Банка, если Клиент не устраняет нарушения условий настоящего Договора.
10.4. Банк вправе расторгнуть настоящий Договор в одностороннем порядке в следующих случаях:
10.4.1. Клиент не подключился к Системе в течение 30 дней с момента заключения Договора.
10.4.2. В случае, если Клиент в течение одного месяца не оплатил стоимость услуг Банка.
10.4.3. В иных случаях, предусмотренных законодательством, нормативными актами НБТ и настоящим Договором.

11. АНТИКОРРУПЦИОННЫЕ ТРЕБОВАНИЯ

11.1. Стороны обязуются безоговорочно соблюдать требования законодательства Республики Таджикистан по борьбе с коррупцией. Стороны осознают и подтверждают, что существует уголовная, административная, гражданско-правовая и дисциплинарная ответственность за совершение коррупционных действий.
11.2. Каждая Сторона настоящего Договора гарантирует и подтверждает, что ни сама сторона, ни её руководство, или работники, ни иные их ответственные лица не предлагали/не требовали/не обещали денежные средства, ценные бумаги, какие-либо привилегии или иные ценные вещи в целях заключения договора и его действия. Стороны обязуются в течение всего срока действия настоящего Договора и после его истечения принимать необходимые меры по недопущению совершения коррупционных действий.
11.3. В случае возникновения у Стороны подозрений, что произошло или может произойти нарушение каких-либо положений пунктов 11.1. и 11.2. настоящего Договора, соответствующая Сторона обязуется уведомить об этом другую Сторону в письменной форме. В случае возникновения сомнений, Клиент может связаться с банком по электронной почте **anticorruption@eskhata.tj**.
11.4. В случае нарушения вышеуказанных требований одной Стороной другая Сторона вправе в одностороннем порядке расторгнуть договор.

12. ПРОЧИЕ УСЛОВИЯ ДОГОВОРА

12.1 В случае выявления несовместимости технических и программных средств или обнаружения низкого качества связи, что делает невозможным обеспечение функционирования Системы, Банк предоставляет рекомендации по организации рабочего места. В соответствии с этими рекомендациями Клиент обязан принять меры по созданию благоприятных условий для работы Системы.
12.2 Если обмен данными становится невозможным из-за отключения электроэнергии, неисправности оборудования Банка или Клиента, банковские операции осуществляются в обычном порядке в соответствии с условиями договора банковского счета.
12.3. Стоимость регистрации/установки, абонентской платы (ежемесячно), а также платы за любые дополнительные услуги, связанные с процессом регистрации и использования Системы, определяется Тарифами Банка.
12.4. Клиент может связаться с соответствующим отделом обслуживания клиентов Банка, позвонив по

телефону **+992 44 6000600** или по короткому номеру **808.**

12.5. Для Клиентов, которые до вступления в силу настоящего Договора заключили с Банком договор об оказании дистанционных банковских услуг с использованием системы «интернет-банкинг» или иного вида договора об оказании дистанционных банковских услуг и в рамках этих договоров Банк продолжает предоставлять такие услуги, настоящий Договор (публичная оферта) считается новой редакцией действующих договоров, при условии, что Клиент предоставит Банку заявление-запрос установленной формы (Приложение №1/1).

12.6. Все иные условия и требования, не предусмотренные настоящим Договором, регулируются в соответствии с требованиями действующего законодательства Республики Таджикистан.

12.7. **Приложения:**

Приложение № 1- Заявление-заявка на подключение к Системе.

Приложение №1/1- Заявление-запрос о присоединении к оферте для действующих клиентов.

Приложение № 2- Запрос на изменение логина и пароля.

Приложение № 3 - Правила проведения экспертизы в случае возникновения споров.

Приложение № 4 - Правила информационной безопасности при работе в системе дистанционного банковского обслуживания «Эсхата Бизнес».

13. ИНФОРМАЦИЯ О БАНКЕ:

Открытое акционерное общество «Банк Эсхата» (Головной офис)

Лицензия Национального банка Таджикистана на осуществление банковских операций от 20 мая 2010 года.

Срок действия лицензии – бессрочная.

Адрес: 735700, Республика Таджикистан, г. Худжанд, улица Гагарина 135

Информационная служба (Контакт-центр): 808

Корреспондентский счет: 20402972457071

ЕИН: 5110001371

ИНН: 510004229

БИК: 350501707

СВИФТ: EJSATJ22

ПРИЛОЖЕНИЕ №1 к Договору
о дистанционному банковскому обслуживании
юридических лиц и индивидуальных предпринимателей
в ОАО «Банк Эсхата» (Публичная оферта)

«____» _____ 20__ г. г. _____

ЗАЯВЛЕНИЕ-ЗАЯВКА

Просим разрешить нашей организации подключиться к дистанционному банковскому обслуживанию для управления депозитными счетами до востребования, открытыми в ОАО «Банк Эсхата», и иными операциями, доступными в Дистанционной системе.

Наименование организации	
ИНН	
Секретное слово	

Пользователи системы дистанционного обслуживания «Эсхата Бизнес»:

ФИО	Должность	E-mail*	Мобильный телефон*
Руководитель *(право первой подписи)*			
Главный бухгалтер/ Бухгалтер *(право второй подписи)*			
Помощник бухгалтера без права подписи *(подготовка документов)*			
Контроллер *(только для просмотра данных)*			

* ***На номера зарегистрированных мобильных телефонов или электронной почты будут отправлены логин и пароль посредством СМС – уведомления.***

Путём подачи настоящего заявления-запроса я акцептую (принимаю) Договор об оказании дистанционного банковского обслуживания для юридических лиц и индивидуальных предпринимателей в ОАО «Банк Эсхата» (ПУБЛИЧНАЯ ОФЕРТА) со всеми его приложениями и подтверждаю, что ознакомлен(а), согласен(на), осознаю положения настоящего Договора (публичной оферты) и его приложений, условия предоставления дистанционных банковских услуг, а также Тарифы Банка, и обязуюсь соблюдать установленные требования при заключении и в период действия договора.Кроме того, получив логин, пароль и секретное слово, я обязуюсь обеспечить их безопасность.

Я, нижеподписавшийся, подтверждаю, что вся вышеуказанная информация является полной и достоверной, а также не возражаю против проведения проверки и обработки предоставленных мной данных.

Я уведомлён и согласен с тем, что могу ознакомиться с Договором дистанционного банковского обслуживания для юридических лиц и индивидуальных предпринимателей в ОАО «Банк Эсхата» (ПУБЛИЧНАЯ ОФЕРТА), а также с его приложениями (включая изменения и дополнения к настоящему Договору или его новую редакцию) и Тарифами Банка по следующим адресам:

- на официальном сайте Банка www.eskhata.com;
- в структурных подразделениях Банка.

СО СТОРОНЫ КЛИЕНТА

_____

(Должность, ФИО и подпись руководителя)

Главный бухгалтер:_____

(ФИО и подпись)

Дата: «___»_____20___

МП

ОТМЕТКА БАНКА:

Данное заявление- заявка было принято Банком.
Предоставленные данные и документы прошли проверку.
Контактный номер телефона и адрес электронной почты для переписки:
Тел: _____ **Email:** _____

Структурное подразделение Банка:_____
(наименование филиала или иного структурного подразделения Банка)

СО СТОРОНЫ БАНКА

_____
(ФИО сотрудника Банка)

_____ Дата: «____»_____20___г.
(подпись)

МП

ПРИЛОЖЕНИЕ №1/1 к Договору
о дистанционному банковскому обслуживании
юридических лиц и индивидуальных предпринимателей
в ОАО «Банк Эсхата» (Публичная оферта)

В ОАО «Банк Эсхата»

От имени ООО «_____»
ИНН:_____
Адрес:_____
_____

ЗАЯВЛЕНИЕ-ЗАПРОС

Прошу Вас разрешить присоединение к Договору дистанционного банковского обслуживания для юридических лиц и индивидуальных предпринимателей в ОАО «Банк Эсхата» (ПУБЛИЧНАЯ ОФЕРТА).

Пользователи системы дистанционного обслуживания «Эсхата Бизнес»:

ФИО	Должность	E-mail*	Мобильный телефон*
Руководитель *(право первой подписи)*			
Главный бухгалтер/ Бухгалтер *(право второй подписи)*			
Помощник бухгалтера без права подписи *(подготовка документов)*			
Контроллер *(только для просмотра данных)*			

* ***На номера зарегистрированных мобильных телефонов или электронной почты будут отправлены логин и пароль посредством СМС – уведомления.***

Путём подачи настоящего заявления-запроса я акцептую (принимаю) Договор об оказании дистанционного банковского обслуживания для юридических лиц и индивидуальных предпринимателей в ОАО «Банк Эсхата» (ПУБЛИЧНАЯ ОФЕРТА) со всеми его приложениями и подтверждаю, что ознакомлен(а), согласен(на), осознаю положения настоящего Договора (публичной оферты) и его приложений, условия предоставления дистанционных банковских услуг, а также Тарифы Банка, и обязуюсь соблюдать установленные требования при заключении и в период действия договора.Кроме того, получив логин, пароль и секретное слово, я обязуюсь обеспечить их безопасность.

Я, нижеподписавшийся, подтверждаю, что вся вышеуказанная информация является полной и достоверной, а также не возражаю против проведения проверки и обработки предоставленных мной данных.

Я уведомлён и согласен с тем, что могу ознакомиться с Договором дистанционного банковского обслуживания для юридических лиц и индивидуальных предпринимателей в ОАО «Банк Эсхата» (ПУБЛИЧНАЯ ОФЕРТА), а также с его приложениями (включая изменения и дополнения к настоящему Договору или его новую редакцию) и Тарифами Банка по следующим адресам:

- на официальном сайте Банка www.eskhata.com;
- в структурных подразделениях Банка.

СО СТОРОНЫ КЛИЕНТА

_____
(Должность, ФИО и подпись руководителя)

Главный бухгалтер:_____
(ФИО и подпись)

Дата: «___»_____20___

МП

Клиент и Банк договорились, что ДОГОВОР №_____ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ «ИНТЕРНЕТ-БАНКИНГ», заключённый между Банком и Клиентом с «» _____ *20* года, считается расторгнутым с даты подписания настоящего Заявления-запроса.

Дальнейшее дистанционное банковское обслуживание между Банком и Клиентом, а также возникающие права и обязательства регулируются Договором дистанционного банковского обслуживания для юридических лиц и индивидуальных предпринимателей в ОАО «Банк Эсхата» (ПУБЛИЧНАЯ ОФЕРТА) и его приложениями.

ОТМЕТКА БАНКА:

Данное заявление- заявка было принято Банком.
Предоставленные данные и документы прошли проверку.
Контактный номер телефона и адрес электронной почты для переписки:
Тел: _____ Email: _____

Структурное подразделение Банка: _____
(наименование филиала или иного структурного подразделения Банка)

СО СТОРОНЫ БАНКА

_____
(ФИО сотрудника Банка)

_____ Дата: «____»_____20___г.
(подпись)
МП

ПРИЛОЖЕНИЕ № 2 к Договору
О дистанционному банковскому обслуживании
юридических лиц и индивидуальных предпринимателей
в ОАО «Банк Эсхата» (Публичная оферта)

«____» _____ 20__г. г._____

ЗАЯВКА

(На смену логина и пароля для входа в Дистанционную систему)

Просим Вас разрешить сотрудникам нашей организации сменить логин и пароль для входа в Дистанционную систему.

Наименование организации	
ИНН	

Пользователи Системы дистанционного банковского обслуживания, логины и пароли которых необходимо изменить

ФИО	Должность	E-mail	Мобильный телефон*
Руководитель *(право первой подписи)*			
Главный бухгалтер/ Бухгалтер *(право второй подписи)*			
Помощник бухгалтера без права подписи *(подготовка документов)*			
Контроллер *(только для просмотра данных)*			
Информация о причине смены логина/пароля (потеря, смена руководства и т.д.)			

* *Логин и пароль будут отправлены на зарегистрированные номера мобильных телефонов по СМС или на электронную почту.*

Путём подачи настоящего заявления-запроса я акцептую (принимаю) Договор об оказании дистанционного банковского обслуживания для юридических лиц и индивидуальных предпринимателей в ОАО «Банк Эсхата» (ПУБЛИЧНАЯ ОФЕРТА) со всеми его приложениями и подтверждаю, что ознакомлен(а), согласен(на), осознаю положения настоящего Договора (публичной оферты) и его приложений, условия предоставления дистанционных банковских услуг, а также Тарифы Банка, и обязуюсь соблюдать установленные требования при заключении и в период действия договора. Кроме того, получив логин, пароль и секретное слово, я обязуюсь обеспечить их безопасность.

КЛИЕНТ **БАНК**

_____ _____

(Должность и ФИО руководителя организации) (ФИО сотрудника Банка)

_____ _____

(подпись) (подпись)

МП МП

Главный бухгалтер:_____

_____

(подпись)

Правила
проведения экспертизы в случае возникновения споров

1. В процессе отправки и получения электронных документов через Систему могут возникать споры при составлении, передаче, принятии и подтверждении получения электронных документов, а также при использовании данных документов с аналогом собственноручной подписи или простой электронной подписи. Споры также могут возникнуть в следующих ситуациях:
1.1. подлинность электронных документов не удостоверена аналогом собственноручной подписи или простой электронной подписью получающей стороны;
1.2. заявление Стороны об искажении электронного документа;
1.3. оспаривание факта отправки/получения электронных документов;
1.4. оспаривание времени отправки/получения электронных документов;
1.5. оспаривание верности копий электронных документов и/или оригинала и второго экземпляра бумажного документа;
1.6. иные случаи споров, связанных с использованием Системы.
2. В случае возникновения спора, Сторона, которой стало известно о возникновении такой ситуации, обязана незамедлительно, но не позднее 3 дней с момента возникновения такого спора, сообщить об этом другой Стороне посредством уведомления.
3. Уведомление о спорной ситуации должно содержать информацию о характере спора и фактах, подтверждающих возможность его возникновения с точки зрения уведомителя, а также претензии к другой стороне. В уведомлении указываются фамилия, имя, отчество, должность, номер телефона, номер факса, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию спора. Уведомление составляется и направляется в форме электронного документа, при невозможности - в форме бумажного документа с подтверждением его получения.
4. Сторона, которой направлено уведомление о споре, обязана незамедлительно, но не позднее следующего рабочего дня, проверить наличие спорных ситуаций и сообщить направившей уведомление Стороне о результатах проверки и, при необходимости, о принятых мерах по урегулированию спора.
5. После получения информации отправителем:
5.1 Споры считаются разрешенными, если отправитель удовлетворен полученной информацией и отказывается от претензий, изложенных в уведомлении.
5.2 В случае его неудовлетворенности для разрешения споров создается экспертная комиссия (далее - Комиссия).
6. В состав Комиссии входят не менее двух представителей Банка и представитель(и) Клиента.
7. Созданная Комиссия при рассмотрении споров на технологическом уровне определяет наличие или отсутствие обстоятельств, подтверждающих факт и время отправки электронных документов, их подлинность, а также надлежащее подписание электронных документов аналогом собственноручной подписи или простой электронной подписью, а также идентичность отправленных и полученных документов.
8. Комиссия имеет право рассматривать другие технические вопросы, которые она сочтет необходимыми для определения причин и последствий споров.
9. Все действия Комиссии, направленные на установление истинных обстоятельств возникновения спорной ситуации, а также выводы Комиссии отражаются в протоколе экспертной Комиссии.
Данный протокол является основным документом работы Комиссии и подписывается всеми членами Комиссии.
10. Проверка наличия или отсутствия обстоятельств, подтверждающих факт и время отправки электронных документов, осуществляется с участием компании, предоставляющей услуги связи между Банком и Клиентом.
11. Проверка подлинности аналога собственноручной подписи или простой электронной подписи в электронных документах осуществляется Комиссией посредством Системы.
11.1 При удостоверении аналога собственноручной подписи или простой электронной подписи символы логин и пароля и/или авторизационных данных, указанном в протоколе проверки, сравниваются с символами простой электронной подписи бумажных экземпляров, подписанных Банком. Если символы совпадают, подлинность подписи Стороны-отправителя электронного документа считается подтвержденной. В случае отрицания Стороной-отправителем электронных документов факта отправки, Комиссия может принять решение о компрометации логин и пароля (простой электронной подписи) Стороны-отправителя электронных документов, не признающей подлинность отправленных электронных документов.

11.2 При отрицательном результате проверки аналога собственноручной подписи или простой электронной подписи Стороны, отправляющей электронные документы, Комиссия принимает решение о том, что указанная Сторона не отправляла электронные документы другой Стороне. Спорный документ признается недействительным.

12. Итоги работы Комиссии оформляются в виде Акта, который подписывается всеми членами Комиссии и направляется каждой стороне. Акт должен содержать следующую информацию:

12.1. обстоятельства, вызвавшие спор;

12.2. протокол работы Комиссии;

12.3. выводы Комиссии.

13. Если предложение Банка о создании Комиссии остается без ответа или отклоняется Клиентом, или Клиент препятствует работе Комиссии, Банк вправе предпринять такие действия в одностороннем порядке, указав основания для таких действий. В Акте указываются основания для вывода о подлинности (поддельности, принятии, отправке, отзыве и т.д.) спорных электронных документов. Такой Акт составляется в двух экземплярах, подписывается Банком, и один экземпляр направляется Клиенту по почте.

14. Акт Комиссии является основанием для принятия решения по спорным вопросам.

15. Стороны признают, что Акт, составленный Комиссией, имеет обязательную силу для Сторон и может быть использован в качестве доказательства в ходе судебных споров. В случае невозможности урегулирования споров путем переговоров и неисполнения решений Комиссии в добровольном порядке, материалы могут быть направлены в суд.

Правила
информационной безопасности при работе в системе дистанционного банковского обслуживания «Эсхата Бизнес»

Правила информационной безопасности при работе в системе дистанционного банковского обслуживания "Эсхата Бизнес" (далее – Правила) составлены в соответствии с требованиями Законодательства РТ, и другими нормативными документами НБТ, а также Политикой информационной безопасности ОАО «Банк Эсхата» и являются обязательными к исполнению Клиентами, заключившими Договор о дистанционном банковском обслуживании юридических лиц и индивидуальных предпринимателей в ОАО «Банк Эсхата» (далее – ДБО).

1. Общие положения

1.1. Настоящие Правила являются обязательным Приложением к «Договора о дистанционном банковском обслуживании юридических лиц и индивидуальных предпринимателей в ОАО «Банк Эсхата» и является неотъемлемой его частью..

1.2. Настоящие Правила определяют Защитные меры по обработке Рисков нарушения Информационной безопасности при использовании Клиентами Системы ДБО. При этом Клиент обязан учитывать то, что:

- Сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;
- Существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Интернет;
- Существует вероятность атаки Злоумышленников на оборудование, программное обеспечение и информационные ресурсы Клиента, подключенные/доступные из сети Интернет;
- Гарантии по обеспечению Информационной безопасности при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются;
- Меры по нейтрализации Злоумышленных действий могут быть эффективными только в течение первых часов после Инцидента;
- Расследованием Злоумышленных действий и поиском Злоумышленников занимаются правоохранительные органы. В целях проведения расследования пострадавшая сторона должна предоставить в распоряжение следственных органов компьютер, который использовался для доступа в Систему, для проведения экспертизы.

1.3. Термины и определения, используемые в настоящем документе:

- **Google Authenticator** - программа обеспечивает двухфакторную аутентификацию для удаленного входа в систему и простых электронных подписей электронных документов с использованием алгоритмов одноразового пароля на основе времени (TOTP) и одноразового пароля на основе HMAC (HOTP). Эта программа реализует алгоритмы, указанные в RFC 6238 и RFC 4226.
- **(2FA)** - метод усиленной безопасности, который требует два различных типа идентификации для подтверждения личности пользователя. Первый фактор — это то, что вы знаете (например, пароль), а второй — то, что у вас есть (например, мобильное устройство с приложением Google Authenticator).
- **Злоумышленник –** нарушитель, действующий намеренно из корыстных, идейных или иных побуждений. **Злоумышленные действия** – любые действия, совершаемые Злоумышленником в Системе.
- **Угроза** - опасность, предполагающая возможность потерь (ущерба).
- **Риск** - мера, учитывающая вероятность реализации Угрозы и величину потерь (ущерба) от реализации этой Угрозы.
- **Информационная безопасность** - безопасность, связанная с Угрозами в информационной сфере. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.
- **Защитная мера** - сложившаяся практика, процедура или механизм, которые используются для уменьшения Риска нарушения Информационной безопасности в Системе.
- **Инцидент** - событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию Угрозы Информационной безопасности
- **Риск нарушения информационной безопасности** - Риск, связанный с Угрозой Информационной безопасности.
- **Обработка риска нарушения информационной безопасности** - процесс выбора и осуществления Защитных мер, снижающих Риск нарушения Информационной безопасности, или мер по переносу, принятию или уходу от Риска.
- **Антивирусная защита** - специализированное программное обеспечение, предназначенное для обнаружения, блокировки и удаления вирусов, вредоносных программ и других угроз безопасности, которые могут заражать мобильные устройства.

- **Защита от фишинга**- меры и технологии, направленные на предотвращение атак, когда злоумышленники пытаются обмануть пользователей, выдавая себя за доверенные организации или лица с целью получения конфиденциальной информации, такой как логины, пароли, номера кредитных карт и другие личные данные.

2. Обязанности сторон

2.1. Обязанности Банка:

- Банк обязуется обеспечить доступность Службы поддержки клиентов Банка (808) для взаимодействия с Клиентами по вопросам предоставления услуг через удаленные каналы обслуживания.
- Банк обязуется предоставить услуги по обслуживанию Клиентов своевременно (сброс пароля, регистрация Клиента) в течении рабочего дня.

2.2. Обязанности клиента:

- Клиент обязан за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые для обмена документами по Системе ДБО.
- Клиент обязуется сохранять в тайне применяемую в Системе ДБО Ключевую информацию.
- Клиент обязуется ознакомиться с мерами безопасности при работе в Системе ДБО, и неукоснительно их соблюдать.
- Клиент соглашается с получением услуг посредством Системы ДБО через сеть Интернет, осознавая, что сеть Интернет не является безопасным каналом связи, и соглашается нести финансовые риски и риски нарушения конфиденциальности, связанные с возможной компрометацией информации при её передаче через сеть Интернет.
- Клиент несет полную ответственность за сохранность и перенос данных Google Authenticator, используемого для доступа к Системе ДБО.
- Обеспечивать сохранность устройства, на котором установлен Google Authenticator.
- Самостоятельно переносить Google Authenticator на новое устройство при необходимости.
- Регулярно проверять и мониторить транзакции в ДБО необходимо для своевременного обнаружения несанкционированных операций или подозрительной активности.

2.3. Банк не несет ответственности:

- за любые, в том числе Злоумышленные, действия третьих лиц в отношении и/или с использованием технических и программных средств, когда-либо использовавшихся Клиентом.
- за сбои в работе электронной почты, сети Интернет, сетей связи, возникшие по не зависящим от Банка причинам и повлекшие за собой несвоевременное получение или неполучение Клиентом уведомлений Банка.
- в случае, если информация Клиента (логин/пароль от Системы ДБО), станет известной иным лицам в результате недобросовестного выполнения Клиентом условий их хранения и использования.
- за потерю доступа к аккаунтам в случае утери или кражи устройства с Google Authenticator.
- некорректную работу Google Authenticator, вызванную действиями Клиента.
- за ненадлежащее исполнение своих обязательств по ДБО в случае, если исполнение оказалось невозможным вследствие обстоятельств непреодолимой силы (т.е. чрезвычайных, непредотвратимых при данных условиях обстоятельств). К таким обстоятельствам относятся, в частности, пожары, стихийные бедствия (землетрясения, наводнение, ураган), массовые заболевания (эпидемии), забастовки, военные действия, террористические акты, диверсии, запрет операций, в том числе с отдельными странами, вследствие принятия международных санкций и другие, не зависящие от воли сторон обстоятельства.
- в случаях невыполнения Клиентом условий ДБО.
- за ущерб и факт разглашения банковской тайны, возникшие вследствие допуска Клиентом третьих лиц к использованию мобильного устройства, номер которого зарегистрирован Клиентом для доступа к Системе ДБО.
- за ущерб, возникший в результате несвоевременного уведомления Банка о прекращении использования номера мобильного телефона.
- Банк фиксирует все действия, совершенные от имени Клиента в электронном журнале Системы ДБО. Содержимое журнала Системы ДБО используется при разрешении спорных ситуаций и предоставляется по запросу правоохранительных органов в целях проведения расследования Злоумышленных действий.

3. Защитные меры при работе в системе ДБО

Банк информирует Клиентов о мерах безопасности при работе в Системе ДБО, рисках Клиента и возможных последствиях для Клиента в случае несоблюдения им мер информационной безопасности, рекомендованных Банком. Информирование осуществляется на сайте Банка или в Подразделениях Банка, или путем отправки SMS-сообщений на номер мобильного устройства Клиента, зарегистрированный для доступа к Системе ДБО, или иными способами, установленным в ДБО.

3.1. Обеспечение безопасности ключевой информации.

- Не сообщайте никому, в том числе сотрудникам банка, логины, пароли доступа, одноразовые пароли к ресурсам Банка. Не сообщайте посторонним лицам, в том числе через сеть интернет, историю операций, контактные и учетные данные, так как эти данные могут быть использованы Злоумышленниками для получения доступа к Вашим счетам.
- Храните в недоступном для третьих лиц месте свои аутентификационные данные.
- При Компрометации или подозрении на Компрометацию пароля доступа – незамедлительно произвести смену пароля в настройках Системы ДБО. При невозможности незамедлительно выполнить указанные выше действия, незамедлительно обратиться в Службу поддержки Банка или любое Подразделение Банка.
- Не используйте одинаковые логин и пароль для доступа к различным системам.

- Регулярно, производите смену Пароля. Пароль должен содержать не менее 10 знаков. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: /; *; -; +; @; &. Настоятельно рекомендуется использовать специализированные программы-генераторы паролей.
- Не используйте в качестве пароля имена, памятные даты, номера телефонов.
- Не храните незашифрованные идентификационные данные на жестком диске, так как эти данные могут быть похищены Злоумышленником и использованы для получения доступа к Вашим счетам.

3.2. Соблюдение общих правил безопасного использования системы ДБО.

- Убедитесь, что устройства, которые вы используете для доступа к ДБО (компьютеры, смартфоны), защищены актуальным антивирусным программным обеспечением и обновленными операционными системами.
- Не рекомендуется использовать чужой компьютер для доступа к Системе ДБО, в случае если доступ к Системе ДБО необходимо осуществить с использованием постороннего компьютера, не рекомендуется сохранять на нем идентификационные данные и другую информацию, а после завершения всех операций нужно убедиться, что идентификационные данные и другая информация не сохранились. После возвращения к штатному персональному компьютеру обязательно смените логин и пароль.
- Всегда явным образом завершайте сеанс работы с Системой ДБО, используя пункт меню «Выход».
- Четко регламентируйте порядок использования компьютера, с которого осуществляется взаимодействие с Системой, в том числе список лиц и порядок доступа к компьютеру. Не рекомендуется использовать указанный компьютер для доступа к посторонним сайтам.
- Отключить функцию «Общие файлы», при использовании компьютера в локальной рабочей сети.
- Настройте механизм информирования о входе в Систему и совершаемых операциях на СМС уведомления. Регулярно проверяйте входящие сообщения, а также журнал операций Системы. Поддерживайте свою контактную информацию в Системе в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.
- В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе ДБО, незамедлительно смените логин и пароль, сообщите об инциденте в Службу поддержки клиентов Банка.

3.3. Соблюдение правил безопасного использования Простой электронной подписи

При использовании ключа ПЭП соблюдайте следующие правила:

- Не передавайте носитель авторизатционных данных третьим лицам, не оставляйте его без присмотра, не храните в доступном месте.
- При получении носителя авторизатционных данных создайте резервную копию, хранимую в сейфе.
- На электронном носителе, на котором расположены логин и парол и/или другие авторизационные данные, не должно быть другой информации.
- Хранение логин и пароль и/или аторизационных данных на жестком диске недопустимо.
- Не позволяйте третьим лицам производить за Вас генерацию пароля.
- Присоединяйте носитель авторизационных данных к компьютеру непосредственно перед началом работы с Системой ДБО. По окончании работы извлекайте носитель из компьютера.
- Незамедлительно проводить замену сертификата проверки логин и пароля при смене должностных лиц, наделенных полномочиями по распоряжению денежными средствами на расчетном счете юридического лица.

3.4. Использование и обновление системного и прикладного ПО.

- Использовать и оперативно обновлять лицензионное системное и прикладное программное обеспечение (ПО) только из доверенных источников, гарантирующих отсутствие вредоносных программ.
- Использовать и оперативно обновлять специализированное ПО для защиты информации - антивирусное ПО. Выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ. В случае обнаружения вирусов (вредоносного программного обеспечения) на компьютере, после его удаления незамедлительно смените логин и пароль в Системе и произведите замену ПЭП.
- Не устанавливайте на компьютере, который используется для взаимодействия с Системой, постороннее программное обеспечение, например, программы автоматического переключения раскладки клавиатуры, различные дополнения к браузерам и т.п. Доказано, что подобные программы передают информацию о содержимом просматриваемых страниц посторонним лицам.
- Не запускайте на своем компьютере программы, полученные из незаслуживающих доверия источников. В случае установки на компьютеры, на которых ведется работа в системе ДБО, программ для удаленной поддержки пользователей (например, TeamViewer, AnyDesk и т.п.), Клиент полностью принимает на себя все риски настроек безопасности доступа в этих программах, передачи третьим лицам.

3.5. Соблюдение правил безопасной работы в сети интернет.

- Не осуществлять вход в Систему ДБО и проведение операций в Системе ДБО с использованием не доверенных (публичных) беспроводных сетей.
- Не используйте функцию запоминания логина и пароля в браузерах.
- Не открывайте подозрительные файлы или ссылки, пришедшие по электронной почте или через сообщения в системе ДБО, так как в них могут быть вирусы (вредоносное программное обеспечение), способные украсть ваши идентификационные данные для входа в Систему и логин и пароль.
- Если Вы получили на электронную почту письмо с просьбой обновить или предоставить какую-либо информацию со ссылкой на какой-либо сайт или телефон (в том числе – сайт Банка), перезвоните в Службу технической поддержки Банка и сообщите о письме. Банк никогда не просит передать данные для входа в ДБО. Обновление данных осуществляется только сотрудником Банка в присутствии представителя Клиента, предъявившего документ,

удостоверяющего личность. Не открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах, и не отвечайте на них.

- Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.
- Настройте браузер на использование протокола защищенной связи TLS. Использование протоколов семейства SSL не обеспечивает надлежащей защиты.
- Перед вводом своего логина и пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверьте правильность указания адреса сайта, наличие сертификата безопасности. В случае обнаружения подозрительных web-сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением официального сайта ОАО «Банк Эсхата», просьба сообщить об этом по телефону 808 или по электронной почте chatcenter@eskhata.tj.

3.6. Соблюдение правил при работе с мобильными устройствами.

- Клиент обязан исключить возможность использования третьими лицами номера мобильного устройства, зарегистрированного для доступа к Системе ДБО. Установите на телефоне/смартфоне пароль для доступа к устройству, данная возможность доступна для любых современных моделей телефонов/смартфонов.
- При потере или краже мобильного устройства, на котором установлено ПО «Google authenticator» для подтверждения электронных операции, необходимо незамедлительно сообщить в Службы поддержки клиентов Банка (808). Только после этого доступ к Системе ДБО будет заблокирован, и злоумышленник не сможет воспользоваться вашим Счетом в Банке.
- Не устанавливайте непроверенные мобильные приложения, в частности с неизвестных источников, на мобильное устройство, на которое установлено ПО «Google authenticator» для подтверждения операций в Системе.
- Установите антивирусное приложение на мобильное устройство, на которое установлено ПО «Google authenticator» для подтверждения операций в Системе.

Клиент обязан информировать Банк о прекращении использования номера мобильного телефона, зарегистрированного для доступа к Системе ДБО, а также о следующих факторах:

- о факте смены абонентского номера Клиента;
- о факте расторжения с оператором связи договора об оказании Клиенту услуг связи по инициативе Клиента;
- о факте наличия вредоносного программного обеспечения на Мобильном устройстве Клиента;
- о факте смены Мобильного устройства Клиента;
- о факте подключенной услуги переадресации вызова и сообщений к абонентскому номеру Клиента.

4. Рекомендации по безопасности и профилактике

- Постоянно следите за новыми методами мошенничества и кибератаками, чтобы быть в курсе текущих угроз.
- Регулярно обновляйте свои знания о методах защиты и современных стандартах безопасности.
- Активно сотрудничайте с Банком и следуйте их рекомендациям по безопасности для минимизации рисков.
- Обращайтесь за консультациями и поддержкой в случае возникновения вопросов или подозрительной активности.
- Внимательно обрабатывайте личную информацию и избегайте предоставления её по ненадёжным каналам связи.Регулярно мониторьте свои финансовые операции и оперативно реагируйте на подозрительные транзакции.